UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/687,193	10/16/2003	Ji Wei Lin	TS01-513	7561

42717 7590 02/22/2007

HAYNES AND BOONE, LLP
901 MAIN STREET, SUITE 3100
DALLAS, TX 75202

EXAMINER	
NGUYEN, MINH DIEU T	
ART UNIT	**PAPER NUMBER**
2137	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/687,193	LIN ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *1/15/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 1-18, 20-27, 30-45 and 48-54 are objected to because of the following informalities:

a) As to claim 1, the phrase "comprising the steps of" should be "comprising steps of"; "converting a recipient's addresses" should be "converting **recipients' addresses**"; "obtaining a recipients public key from encryption software key server" should be "obtaining **recipients' public keys** from **an** encryption software key server"; "using said recipient's encryption software public keys" should be "using said **recipients'** encryption software public keys" and "converting said recipient's address" should be "converting said **recipients' addresses**".

b) As to claims 2-18, the phrase "Public-key encryption software and Email software" should be "an encryption/decryption system and an email platform" for claim consistency since they all depend on the method of claim 1.

c) As to claim 2, the phrase "comprising the steps of" should be "comprising steps of"; "type password of encryption software private key" should be "type password of **an** encryption software private key".

d) As to claim 3, the phrase "comprising the steps of" should be "comprising step of".

e) As to claims 4, 22 and 40, the phrase "conversion of said addresses of said recipients' email addresses" should be "conversion of said recipients' email addresses".

f) As to claims 5, 23 and 41, the phrase "said public keys are obtained from a encryption software server" should be "said **encryption software** public keys are obtained from **an** encryption software server".

g) As to claims 6, 24 and 42, the phrase "wherein said keys are used to encrypt Email software email" should be ""wherein said **encryption software public** keys are used to encrypt Email software email".

h) As to claims 7, 25 and 43, the phrase ""wherein said keys are used to encrypt Email software attachments" should be ""wherein said **encryption software public** keys are used to encrypt Email software attachments".

i) As to claims 8, 26 and 44, the phrase "said Internet addresses are converted back" should be "said **recipients' addresses from said internet format** are converted back".

j) As to claims 9, 27 and 45, the phrase "said conversion of said Internet addresses back to Email software addresses allows the retention of rich text content" should be "said conversion of said **recipients' addresses from said internet format** back to Email **format** allows retention of rich text content".

k) As to claims 12, 30 and 48, the phrase "type in a password of a encryption software private key" should be "type in a password of **an** encryption software private key".

l) As to claim 13, this recited claim depends on claim 1, however the limitation "said encryption software password" is not in claim 1, this limitation is introduced in claim 12, therefore it is suggested that claim 13 depends on claim 12 and

the phrase "wherein said encryption software password and private key are used to decrypt mail content" should be "wherein said encryption software password and private key are used to decrypt **said encrypted email**".

m) As to claim 14, this recited claim depends on claim 1, however the limitation "said encryption software password" is not in claim 1, this limitation is first introduced in claim 12, therefore it is suggested that claim 13 depends on claim 12 and the phrase "wherein said encryption software password and private key are used to decrypt attachment files" should be "wherein said encryption software password and private key are used to decrypt **said encrypted attachment**".

n) As to claim 15, the phrase "said users" should be "users", however this recited claim appears to be the same as claim 3, it is suggested that this claim should be deleted.

o) As to claim 16, this recited claim depends on claim 1, however the limitation "said encryption software key management" is not in claim 1, this limitation is first introduced in claim 3, therefore it is suggested that claim 16 depends on claim 3 and the phrase "changing said password of said encryption software private key" should be "changing password of encryption software private key".

p) As to claim 17, this recited claim depends on claim 1, however the limitation "said encryption software key management" is not in claim 1, this limitation is first introduced in claim 3, therefore it is suggested that claim 17 depends on claim 3.

q) As to claim 18, this recited claim depends on claim 1, however the limitation "said encryption software key management" is not in claim 1, this limitation is

first introduced in claim 3, therefore it is suggested that claim 18 depends on claim 3 and the phrase "sending out said user's encryption software public key" should be "sending out said **users'** encryption software public **keys**".

r) As to claim 20, the phrase "softwareattachments" should be "software attachments"; "type password of encryyption software private key decrypting mail content and decrypting attachment content" should be type password of **an encryption** software private key; **means for decrypting mail content, and means for decrypting attachment content**".

s) As to claim 21, the phrase "comprising the step of" should be "comprising".

t) As to claim 31, this recited claim depends on claim 19, however the limitation "said encryption software password" is not in claim 19, this limitation is introduced in claim 30, therefore it is suggested that claim 31 depends on claim 30 and the phrase "wherein said encryption software password and private key are used to decrypt mail content" should be "wherein said encryption software password and private key are used to decrypt **said encrypted email**".

u) As to claim 32, this recited claim depends on claim 19, however the limitation "said encryption software password" is not in claim 19, this limitation is introduced in claim 30, therefore it is suggested that claim 32 depends on claim 30 and the phrase "wherein said encryption software password and private key are used to decrypt attachment files" should be "wherein said encryption software password and private key are used to decrypt **said encrypted attachment**".

v) As to claim 33, the phrase "said users" should be "users", however this recited claim appears to be the same as claim 21, it is suggested that this claim should be deleted.

w) As to claim 34, this recited claim depends on claim 19, however the limitation "said encryption software key management" is not in claim 19, this limitation is first introduced in claim 21, therefore it is suggested that claim 34 depends on claim 21 and the phrase "changing said password of said encryption software private key" should be "changing password of encryption software private key".

x) As to claim 35, this recited claim depends on claim 19, however the limitation "said encryption software key management" is not in claim 19, this limitation is first introduced in claim 21, therefore it is suggested that claim 35 depends on claim 21.

y) As to claim 36, this recited claim depends on claim 19, however the limitation "said encryption software key management" is not in claim 19, this limitation is first introduced in claim 21, therefore it is suggested that claim 36 depends on claim 21 and the phrase "sending out said user's encryption software public key" should be "sending out said **users'** encryption software public **keys**".

z) As to claim 37, the phrase "performs the steps of" should be "performs step of".

aa) As to claim 38, the phrase "performs the steps of" should be "performs step of", "at least one networked computing deviceof claim 37" should be "at least one networked computing device of claim 37" and "requesting users to type password of

encryption software private key" should be "requesting users to type password of **an** encryption software private key".

ab) As to claim 39, the phrase "comprising the step of" should be "performs step of".

ac) As to claim 49, this recited claim depends on claim 37, however the limitation "said encryption software password" is not in claim 37, this limitation is introduced in claim 48, therefore it is suggested that claim 49 depends on claim 48 and the phrase "wherein said encryption software password and private key are used to decrypt mail content" should be "wherein said encryption software password and private key are used to decrypt **said encrypted email**".

ad) As to claim 50, this recited claim depends on claim 37, however the limitation "said encryption software password" is not in claim 37, this limitation is introduced in claim 48, therefore it is suggested that claim 50 depends on claim 48 and the phrase "wherein said encryption software password and private key are used to decrypt attachment files" should be "wherein said encryption software password and private key are used to decrypt **said encrypted attachment**".

ae) As to claim 51, the phrase "said users" should be "users"; however this recited claim appears to be the same as claim 39, it is suggested that this claim should be deleted.

af) As to claim 52, this recited claim depends on claim 37, however the limitation "said encryption software key management" is not in claim 37, this limitation is first introduced in claim 39, therefore it is suggested that claim 52 depends on claim 39

and the phrase "changing said password of said encryption software private key" should be "changing password of encryption software private key".

ag) As to claim 53, this recited claim depends on claim 37, however the limitation "said encryption software key management" is not in claim 37, this limitation is first introduced in claim 39, therefore it is suggested that claim 53 depends on claim 39.

ah) As to claim 54, this recited claim depends on claim 37, however the limitation "said encryption software key management" is not in claim 37, this limitation is first introduced in claim 39, therefore it is suggested that claim 54 depends on claim 39 and the phrase "sending out said user's encryption software public key" should be "sending out said **users'** encryption software public **keys**".

Appropriate correction is required.

Information Disclosure Statement

2. The information disclosure statement filed 1/15/2004 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 3-8, 10-11, 15, 18-19, 21-26, 28-29, 33, 36-37, 39-44, 46-47, 51 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170).

a) As to claim 1, Meffert discloses a method of integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email (e.g. a secure content delivery system and method for implementing of public key infrastructure (PKI) based encryption and specifically to harnessing the advantages of PKI to provide encryption of and controlled access to data including email, email attachments, see Meffert: 0002) comprising steps of: obtaining recipients' public keys from an encryption software key server (i.e. local agent 130 requests and obtains the necessary keys from control server 200, see Meffert: 0076, a package of encrypted content is generated using PKI-based encryption by obtaining at least one public key from the control server, the encrypted package is sent to the control server, the control server transmits the package to the recipient local agent, the recipient local agent decrypts the encrypted content in the package, see Meffert: Abstract, it is understood that the necessary keys are the recipients' public keys used for encrypting, so then later the recipients' private keys are used for decrypting the encrypted content in the package); using said recipients' encryption software public keys to encrypt an email (i.e. the email content is encrypted with the appropriate keys, see Meffert: 0076); using said recipients' encryption software public keys to encrypt an attachment (i.e. the email and/or any attachments is encrypted using PKI cryptography, see Meffert: 0076). Meffert is silent on the capability of converting recipients' addresses from an email

format to an Internet format and converting recipients' addresses from said Internet format to said email format. Cox is relied on for the teaching of converting recipients' addresses from an email format to an Internet format and converting recipients' addresses from said Internet format to said email format (i.e. domain name system (DNS) server 206 converts the standard e-mail format to a numeric Internet protocol (IP) format, see Cox: 0022). Cox does not explicitly disclose converting said recipients' addresses from said internet format to said email format, however it is well known in the data communications world that the domain name server (DNS) translates domain names (e.g. email) to Internet Protocol address and vice versa. It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of converting recipients' addresses from an email format to an Internet format and converting recipients' addresses from said Internet format to said email format in the system of Meffert, as Cox teaches, so as to make the system simply to use (see Meffert: 0010) by having DNS attachs easy-to-remember domain names (such as "username@postini.com") to hard-to-remember IP addresses (such as 123.45.67.89).

b) As to claim 3, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 further comprising step of allowing users to use a familiar Email software interface to do encryption software key management (i.e. the present invention comprises two main components: a local agent, in conjunction with an application specific interface (ASI) and a control server, these two components can function independently or in combination to allow users to operate existing messaging

software applications, provide the necessary integration to employ PKI-based encryption using that messaging software application and to access application services functionality and PKI certificate and management processes, see Meffert: 0035).

c) As to claim 4, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein said conversion of said recipients' email addresses from Email software format to Internet format is required in order to obtain keys to proceed further (i.e. domain name system (DNS) server 206 converts the standard e-mail format to a numeric Internet protocol (IP) format, see Cox: 0022 and keys are obtained from the control server, see Meffert: 0076).

d) As to claim 5, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein said encryption software public keys are obtained from an encryption software server (i.e. local agent 130 requests and obtains the necessary keys from control server 200, see Meffert: 0076).

e) As to claim 6, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein said encryption software public keys are used to encrypt Email software email (i.e. the email content is encrypted with the appropriate keys (e.g. public keys obtained from the control server, see Meffert: 0076).

f) As to claim 7, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to

encrypt/decrypt email of claim 1 wherein said encryption software public keys are used to encrypt Email software attachments (i.e. the email and/or any attachments is encrypted using PKI cryptography, see Meffert: 0076).

g) As to claim 8, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein said recipients' addresses from said internet format converted back to Email software format to allow email processing using said email software (i.e. the domain name server (DNS) translates domain names (e.g. email) to Internet Protocol address and vice versa to allow email processing, see Cox: 0022).

h) As to claim 10, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein a means is provided for users to read said encryption software encrypted email (i.e. local agent 130 launches a viewer within which the encrypted content including any attached files are decrypted and, thus, viewed, see Meffert: 0074).

i) As to claim 11, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 1 wherein a means is provided for users to read said encryption software encrypted attachments (i.e. local agent 130 launches a viewer within which the encrypted content including any attached files are decrypted and, thus, viewed, see Meffert: 0074).

j) As to claim 15, the limitation of this claim is similar to claim 3 and is rejected by the similar rationale applied against claim 3.

k) As to claim 18, as suggested depending on claim 3, the combination of Meffert and Cox teaches the method for integrating an encryption/decryption system and an email platform in order to encrypt/decrypt email of claim 3 wherein said encryption software key management also includes sending out said users' encryption software public keys to other people (i.e. the electronic delivering statements or bills with component 550 to receive account, public key and certificate data corresponding to each client associated with the billing data, the client billing data and account and certificate data are then packaged together and passed to the high volume encryption component which employs PKI based encryption using the certificate packaged with the billing data and account data, it is understood that the public keys are distributed to other people such as the presentment services, see Meffert: 0095-0096).

l) As to claim 19, this claim is directed to a hardware implementation of method of claim 1 and is rejected by a similar rationale applied against claim 1 above.

m) As to claim 21, this claim is directed to a hardware implementation of method of claim 3 and is rejected by a similar rationale applied against claim 3 above.

n) As to claim 22, this claim is directed to a hardware implementation of method of claim 4 and is rejected by a similar rationale applied against claim 4 above.

o) As to claim 23, this claim is directed to a hardware implementation of method of claim 5 and is rejected by a similar rationale applied against claim 5 above.

p) As to claim 24, this claim is directed to a hardware implementation of method of claim 6 and is rejected by a similar rationale applied against claim 6 above.

q) As to claim 25, this claim is directed to a hardware implementation of method of claim 7 and is rejected by a similar rationale applied against claim 7 above.

r) As to claim 26, this claim is directed to a hardware implementation of method of claim 8 and is rejected by a similar rationale applied against claim 8 above.

s) As to claim 28, this claim is directed to a hardware implementation of method of claim 10 and is rejected by a similar rationale applied against claim 10 above.

t) As to claim 29, this claim is directed to a hardware implementation of method of claim 11 and is rejected by a similar rationale applied against claim 11 above.

u) As to claim 33, this claim is directed to a hardware implementation of method of claim 15 and is rejected by a similar rationale applied against claim 15 above.

v) As to claim 36, as suggested depending on claim 21, this claim is directed to a hardware implementation of method of claim 18 and is rejected by a similar rationale applied against claim 18 above.

w) As to claim 37, this claim is directed to a software implementation of method of claim 1 and is rejected by a similar rationale applied against claim 1 above.

x) As to claim 39, this claim is directed to a software implementation of method of claim 3 and is rejected by a similar rationale applied against claim 3 above.

y) As to claim 40, this claim is directed to a software implementation of method of claim 4 and is rejected by a similar rationale applied against claim 4 above.

z) As to claim 41, this claim is directed to a software implementation of method of claim 5 and is rejected by a similar rationale applied against claim 5 above.

aa) As to claim 42, this claim is directed to a software implementation of method of claim 6 and is rejected by a similar rationale applied against claim 6 above.

ab) As to claim 43, this claim is directed to a software implementation of method of claim 7 and is rejected by a similar rationale applied against claim 7 above.

ac) As to claim 44, this claim is directed to a software implementation of method of claim 8 and is rejected by a similar rationale applied against claim 8 above.

ad) As to claim 46, this claim is directed to a software implementation of method of claim 10 and is rejected by a similar rationale applied against claim 10 above.

ae) As to claim 47, this claim is directed to a software implementation of method of claim 11 and is rejected by a similar rationale applied against claim 11 above.

af) As to claim 51, this claim is directed to a software implementation of method of claim 15 and is rejected by a similar rationale applied against claim 15 above.

ag) As to claim 54, as suggested depending on claim 39, this claim is directed to a software implementation of method of claim 18 and is rejected by a similar rationale applied against claim 18 above.

5. Claims 2, 12-14, 20, 30-32, 38 and 48-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170) and further in view of applicant admitted prior art (AAPA).

a) As to claim 2, the combination of Meffert and Cox discloses the method of claim 1 further comprising steps of providing a means for users to read encryption software encrypted email and email attachments (i.e. local agent 130 launches a viewer within which the encrypted content including any attached files are decrypted and, thus, viewed, see Meffert: 0074), however it is silent of the capability of requesting users to type password of an encryption software private key. The applicant admitted prior art (AAPA) discloses requesting users to type password of an encryption software private key (see AAPA: 0006). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of requesting users to type password of an encryption software private key in the system of Meffert and Cox, as AAPA discloses, so as to provide robust security and identity authentication with respect to content delivered over the Internet (see Meffert: 0010).

b) As to claim 12, the combination of Meffert and Cox discloses the method of claim 1, however it is silent on the capability of requesting users to type in a password of an encryption software private key. The applicant admitted prior art (AAPA) discloses requesting users to type in a password of an encryption software private key (see AAPA: 0006). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of requesting users to type in a password of an encryption software private key in the system of Meffert and Cox, as AAPA discloses, so as to provide robust security and identity authentication with respect to content delivered over the Internet (see Meffert: 0010).

c) As to claim 13, as suggested depending on claim12, the combination of Meffert, Cox and AAPA discloses the method of claim 12 wherein said encryption software password and private key are used to decrypt mail content (i.e. the typed in password is used to decrypt mail content, see AAPA: 0006 and private key in the public/private key pair is used for decrypt mail content, see Meffert: 0006).

d) As to claim 14, as suggested depending on claim12, the combination of Meffert, Cox and AAPA discloses the method of claim 12 wherein said encryption software password and private key are used to decrypt attachment files (i.e. the typed in password is used to decrypt attachment files, see AAPA: 0006 and private key in the public/private key pair is used for decrypt attachment files, see Meffert: 0006).

e) As to claim 20, this claim is directed to a hardware implementation of method of claim 2 and is rejected by a similar rationale applied against claim 2 above.

f) As to claim 30, this claim is directed to a hardware implementation of method of claim 12 and is rejected by a similar rationale applied against claim 12 above.

g) As to claim 31, as suggested depending on claim 30, this claim is directed to a hardware implementation of method of claim 13 and is rejected by a similar rationale applied against claim 13 above.

h) As to claim 32, as suggested depending on claim 30, this claim is directed to a hardware implementation of method of claim 14 and is rejected by a similar rationale applied against claim 14 above.

i) As to claim 38, this claim is directed to a software implementation of method of claim 2 and is rejected by a similar rationale applied against claim 2 above.

j) As to claim 48, this claim is directed to a software implementation of method of claim 12 and is rejected by a similar rationale applied against claim 12 above.

k) As to claim 49, as suggested depending on claim 48, this claim is directed to a software implementation of method of claim 13 and is rejected by a similar rationale applied against claim 13 above.

l) As to claim 50, as suggested depending on claim 48, this claim is directed to a software implementation of method of claim 14 and is rejected by a similar rationale applied against claim 14 above.

6. Claims 9, 27 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170) and further in view of Wolf et al. (5,818,447).

a) As to claim 9, the combination of Meffert and Cox discloses the method of claim 1, particularly converting recipients addresses from said Internet format back to Email format (see Cox: 0022), however it is silent on the capability of having conversion allows retention of rich text content. Wolf is relied on for the teaching of having conversion of said recipients addresses from said Internet format back to Email format allows retention of rich text content (i.e. Wolf discloses a system and method for handling email, see Wolf: col. 1, lines 6-10, Wolf acknowledges rich text capabilities in the email program, see Wolf: col. 1, lines 36-37, and discloses a system that provide sophisticated formatting and editing options in the context of email environment that is compatible with downlevel (rich text) email clients, see Wolf: col. 2, lines 2-5, in

particular, the MAPI formats ensures the interoperability between an embodiment of the present invention, a prior art rich text mail client and other mail clients and gateways, see Wolf: col. 16, lines 29-32). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having conversion of said recipients addresses from said Internet format back to Email format allows retention of rich text content in the system of Meffert and Cox, as Wolf teaches, so as to provide a system for creating sophisticated documents for transmission via electronic email (see Wolf: col. 1, line 67 to col. 2, line 1).

b) As to claim 27, this claim is directed to a hardware implementation of method of claim 9 and is rejected by a similar rationale applied against claim 9 above.

c) As to claim 45, this claim is directed to a software implementation of method of claim 9 and is rejected by a similar rationale applied against claim 9 above.

7. Claims 16, 34 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002/0059144) in view of Cox et al. (2005/0044170) and further in view of Goldstone (2003/0142364).

a) As to claim 16, as suggested depending on claim 3, the combination of Meffert and Cox discloses the method of claim 3, however it is silent on the capability of having encryption software key management includes changing password of an encryption software private key. Goldstone is relied on for the teaching of having encryption software key management includes changing password of an encryption software private key (i.e. the key pair could be changed frequently and the password

required to access the private key could also be changed even more frequently, see Goldstone: 0052). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having encryption software key management includes changing password of an encryption software private key in the system of Meffert and Cox, as Goldstone teaches, so as to provide robust security and identity authentication with respect to content delivered over the Internet (see Meffert: 0010).

b) As to claim 34, as suggested depending on claim 21, this claim is directed to a hardware implementation of method of claim 16 and is rejected by a similar rationale applied against claim 16 above.

c) As to claim 52, as suggested depending on claim 37, this claim is directed to a software implementation of method of claim 16 and is rejected by a similar rationale applied against claim 16 above.

8. Claims 17, 35 and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Meffert et al. (2002//0059144) in view of Cox et al. (2005/0044170) and further in view of Smith et al. (6,651,166).

a) As to claim 17, as suggested depending on claim 3, the combination of Meffert and Cox discloses the method of claim 3, however it is silent on the capability of having encryption software key management includes registering other encryption software public keys with said encryption software key server. Smith is relied on for the teaching of having encryption software key management includes registering other encryption software public keys with said encryption software key server (i.e. register

public key with a trusted authority, see Smith: col. 2, lines 33-35). It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of having encryption software key management includes registering other encryption software public keys with said encryption software key server in the system of Meffert and Cox, as Smith discloses, so as to securely deliver electronic documents to remote recipients (see Smith: col. 1, lines 5-10).

b) As to claim 35, as suggested depending on claim 21, this claim is directed to a hardware implementation of method of claim 17 and is rejected by a similar rationale applied against claim 17 above.

c) As to claim 53, as suggested depending on claim 37, this claim is directed to a software implementation of method of claim 17 and is rejected by a similar rationale applied against claim 17 above.

Conclusion

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published

applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
2/20/07